

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-247022
 (43)Date of publication of application : 30.08.2002

(51)Int.Cl. H04L 9/08
 H04H 1/00

(21)Application number : 2001-046708 (71)Applicant : NIPPON TELEGR & TELEPH CORP
 <NTT>

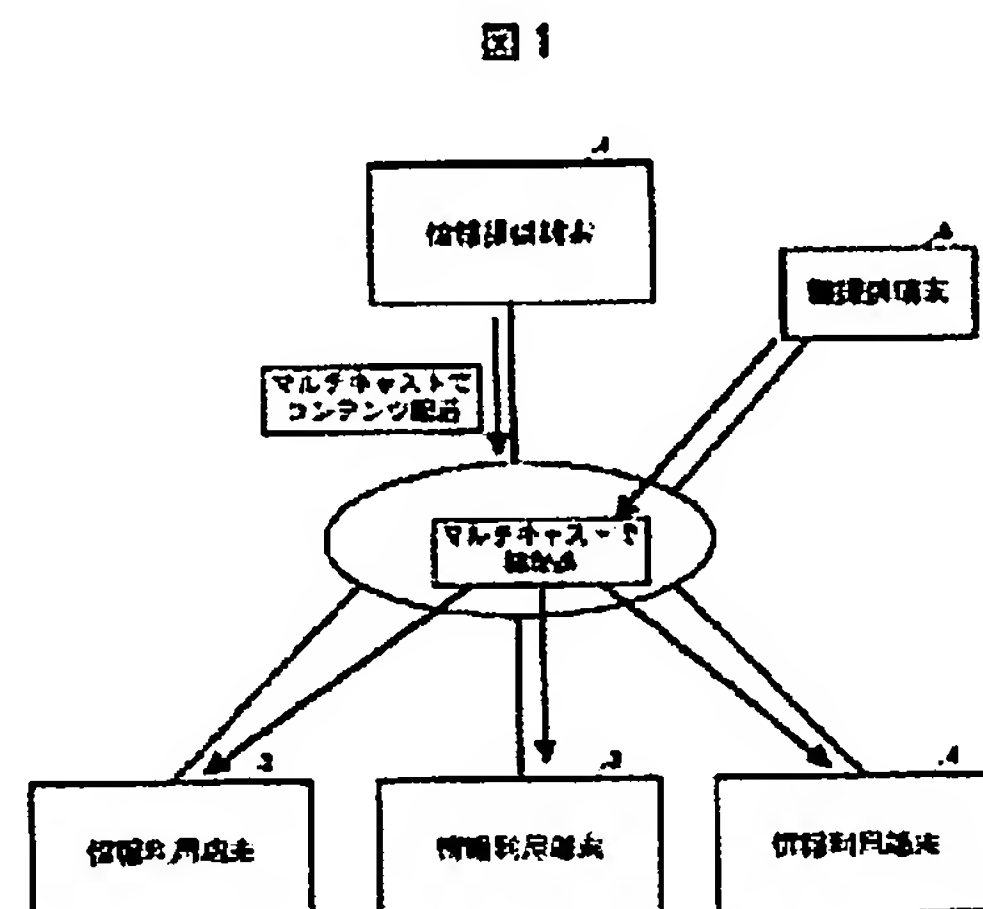
(22)Date of filing : 22.02.2001 (72)Inventor : IORI SACHIKO
 MIYAKE NOBUHISA
 NAKAZATO KANA

(54) METHOD FOR DELIVERING INFORMATION, METHOD FOR UTILIZING INFORMATION, THEIR EXECUTION DEVICE AND PROCESSING PROGRAM, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide technology capable of efficiently delivering a key for deciphering ciphered contents to plural information using terminals.

SOLUTION: The information delivering method for delivering contents from an information providing terminal to plural information using terminals by a multicast state is provided with a step for generating a key for ciphering or deciphering contents, a step for generating ciphered key data obtained by ciphering the key, a step for delivering the generated ciphered key data to respective information using terminals by the multicast state, a step for ciphering the contents by the generated key, and a step for delivering the ciphered contents to respective information using terminals by the multicast state.



(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号
特開2002-247022
(P2002-247022A)

(43)公開日 平成14年8月30日(2002.8.30)

(51)Int.Cl. ⁷	識別記号	F I	テ-マ-ト*(参考)
H 0 4 L 9/08		H 0 4 H 1/00	F 5 J 1 0 4
H 0 4 H 1/00		H 0 4 L 9/00	6 0 1 B
			6 0 1 A

審査請求 未請求 請求項の数19 O L (全 12 頁)

(21)出願番号 特願2001-46708(P2001-46708)

(22)出願日 平成13年2月22日(2001.2.22)

(71)出願人 000004226

日本電信電話株式会社
東京都千代田区大手町二丁目3番1号

(72)発明者 庵 祥子

東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

(72)発明者 三宅 延久

東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

(74)代理人 100083552

弁理士 秋田 収喜

最終頁に続く

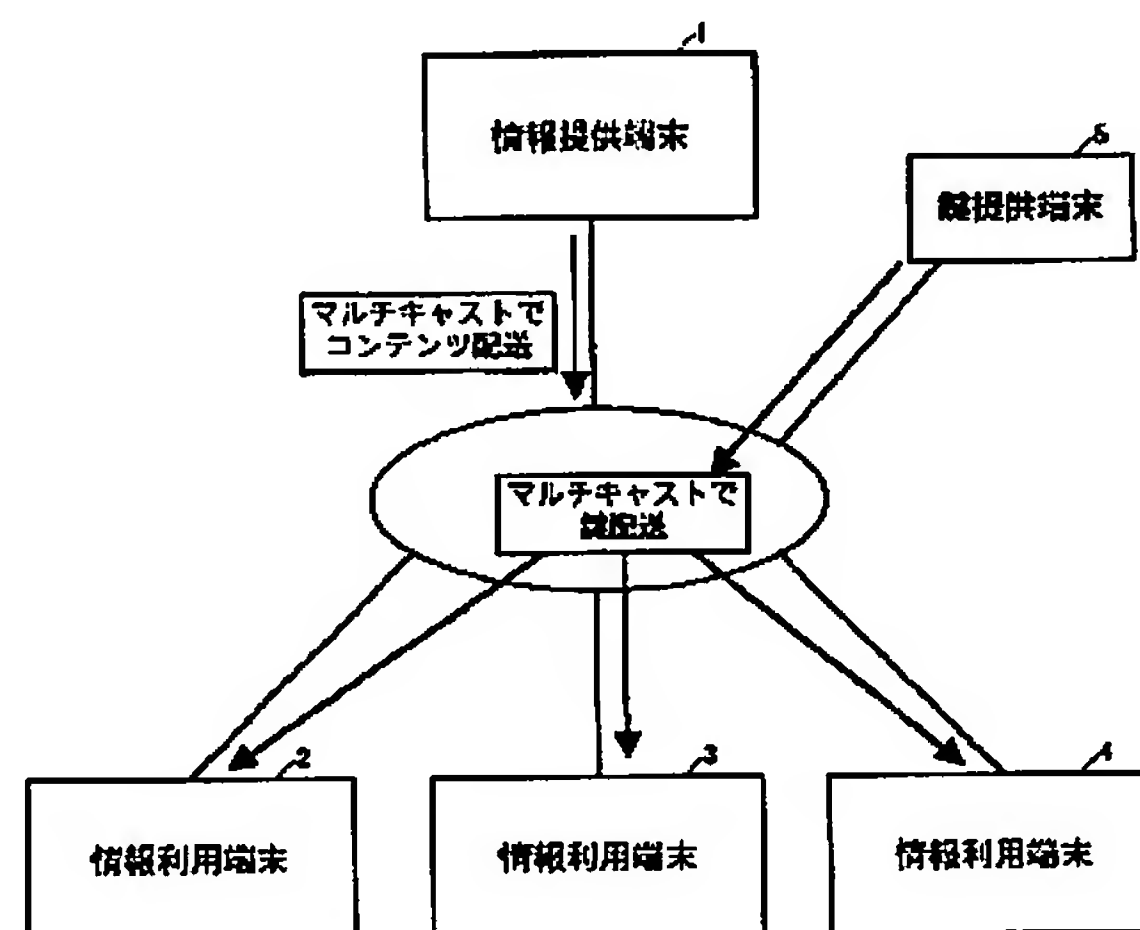
(54)【発明の名称】 情報配送方法、情報利用方法及びその実施装置並びにその処理プログラムと記録媒体

(57)【要約】

【課題】 暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能な技術を提供する。

【解決手段】 コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送方法において、コンテンツを暗号化または復号化する為の鍵を生成するステップと、前記鍵を暗号化して暗号化鍵データを生成するステップと、前記生成した暗号化鍵データをマルチキャストで各情報利用端末に配送するステップと、前記生成した鍵によりコンテンツを暗号化するステップと、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するステップとを有するものである。

図 1



【特許請求の範囲】

【請求項 1】 コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送方法において、

コンテンツを暗号化または復号化する為の鍵を生成するステップと、前記鍵を暗号化して暗号化鍵データを生成するステップと、前記生成した暗号化鍵データをマルチキャストで各情報利用端末に配送するステップと、前記生成した鍵によりコンテンツを暗号化するステップと、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するステップとを有することを特徴とする情報配送方法。

【請求項 2】 暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を各情報利用端末に配送するステップと、変更後の鍵の再配送要求を情報利用端末から受付けるステップと、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データを再配送するステップとを有することを特徴とする請求項 1 に記載された情報配送方法。

【請求項 3】 暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の 2 つ以上のデータを同一のマルチキャストで各情報利用端末に配送することを特徴とする請求項 1 または請求項 2 のいずれかに記載された情報配送方法。

【請求項 4】 マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用方法において、利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データをマルチキャストで取得するステップと、前記取得した暗号化鍵データを保存するステップと、暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するステップと、前記保存した暗号化鍵データを復号化して鍵を生成するステップと、前記取得した暗号化コンテンツを前記生成した鍵で復号化するステップと、前記復号化したコンテンツを再生するステップとを有することを特徴とする情報利用方法。

【請求項 5】 暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を取得するステップと、前記取得した鍵変更予告で予告された変更後の鍵を取得しているかどうかを確認するステップと、前記変更後の鍵を取得していない場合にその変更後の鍵の再配送を要求するステップと、前記再配送を要求した変更後の暗号化鍵データを取得するステップとを有することを特徴とする請求項 4 に記載された情報利用方法。

【請求項 6】 暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の 2 つ以上のデータを同一のマルチキャストにより取得するこ

とを特徴とする請求項 4 または請求項 5 のいずれかに記載された情報利用方法。

【請求項 7】 コンテンツを暗号化または復号化する為の鍵を提供する鍵提供端末において、

コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、前記鍵を暗号化して暗号化鍵データを生成する鍵暗号化部と、前記生成した暗号化鍵データをマルチキャストで各情報利用端末に配送する鍵配送部とを備えることを特徴とする鍵提供端末。

【請求項 8】 暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を各情報利用端末に配送する鍵変更予告配送部と、変更後の鍵の再配送要求を情報利用端末から受付ける鍵再配送受付部と、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データを再配送する鍵再配送部とを備えることを特徴とする請求項 7 に記載された鍵提供端末。

【請求項 9】 マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用端末において、利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データをマルチキャストで取得する鍵取得部と、前記取得した暗号化鍵データを保存する鍵保存部と、暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するコンテンツ取得部と、前記保存した暗号化鍵データを復号化して鍵を生成する鍵復号化部と、前記取得した暗号化コンテンツを前記生成した鍵で復号化するコンテンツ復号化部と、前記復号化したコンテンツを再生するコンテンツ再生部とを備えることを特徴とする情報利用端末。

【請求項 10】 暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を取得する鍵変更予告取得部と、前記取得した鍵変更予告で予告された変更後の鍵を取得しているかどうかを確認する鍵確認部と、前記変更後の鍵を取得していない場合にその変更後の鍵の再配送を要求する鍵再配送要求部と、前記再配送を要求した変更後の暗号化鍵データを取得する鍵再取得部とを備えることを特徴とする請求項 9 に記載された情報利用端末。

【請求項 11】 暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の 2 つ以上のデータを同一のマルチキャストにより取得することを特徴とする請求項 9 または請求項 10 のいずれかに記載された情報利用端末。

【請求項 12】 コンテンツをマルチキャストで情報利用端末に提供する情報提供端末において、利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末から取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化

コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の2つ以上のデータを同一のマルチキャストで各情報利用端末に配送するコンテンツ配送部とを備えることを特徴とする情報提供端末。

【請求項13】 コンテンツを暗号化または復号化する為の鍵を提供する鍵提供端末としてコンピュータを機能させる為のプログラムにおいて、コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、前記鍵を暗号化して暗号化鍵データを生成する鍵暗号化部と、前記生成した暗号化鍵データをマルチキャストで各情報利用端末に配送する鍵配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項14】 暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を各情報利用端末に配送する鍵変更予告配送部と、変更後の鍵の再配送要求を情報利用端末から受け付ける鍵再配送受付部と、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データを再配送する鍵再配送部としてコンピュータを機能させることを特徴とする請求項13に記載されたプログラム。

【請求項15】 マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用端末としてコンピュータを機能させる為のプログラムにおいて、利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データをマルチキャストで取得する鍵取得部と、前記取得した暗号化鍵データを保存する鍵保存部と、暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するコンテンツ取得部と、前記保存した暗号化鍵データを復号化して鍵を生成する鍵復号化部と、前記取得した暗号化コンテンツを前記生成した鍵で復号化するコンテンツ復号化部と、前記復号化したコンテンツを再生するコンテンツ再生部としてコンピュータを機能させることを特徴とするプログラム。

【請求項16】 暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を取得する鍵変更予告取得部と、前記取得した鍵変更予告で予告された変更後の鍵を取得しているかどうかを確認する鍵確認部と、前記変更後の鍵を取得していない場合にその変更後の鍵の再配送を要求する鍵再配送要求部と、前記再配送を要求した変更後の暗号化鍵データを取得する鍵再取得部としてコンピュータを機能させることを特徴とする請求項15に記載されたプログラム。

【請求項17】 暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の2つ以上のデータを同一のマルチキャストにより取得することを特徴とする請求項15または請求項16のいずれ

かに記載されたプログラム。

【請求項18】 コンテンツをマルチキャストで情報利用端末に提供する情報提供端末としてコンピュータを機能させる為のプログラムにおいて、利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末から取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の2つ以上のデータを同一のマルチキャストで各情報利用端末に配送するコンテンツ配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項19】 請求項13乃至請求項18のいずれか1項に記載されたプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンテンツをマルチキャストで配送する情報配送システムに関し、特にストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで配送された復号鍵で復号化することにより情報の利用制御を可能とする情報配送システムに適用して有効な技術に関するものである。

【0002】

【従来の技術】従来、複数の利用者に対してストリームコンテンツ等の同一のコンテンツを提供する場合、マルチキャストを用いることにより効率良くコンテンツの配送を行うことができる。このマルチキャストを用いたコンテンツの配送では、利用者がマルチキャストアドレスを指定することにより、誰でも簡単にそのコンテンツを利用することができる。

【0003】また前記マルチキャストを用いて、利用資格を有する特定の利用者向けにコンテンツを提供しようとする場合には、そのコンテンツを利用者のみが復号できる状態で（例えば利用者に予め配られている鍵を利用する等）暗号化し、その暗号化コンテンツをマルチキャストで配送するという手法がある。利用者は、マルチキャストアドレスを指定して受信した暗号化コンテンツを、予め配られている鍵で復号化することにより、そのコンテンツを利用することができる。

【0004】

【発明が解決しようとする課題】前記従来技術でマルチキャストを用いて暗号化すること無くコンテンツの配送を行った場合、マルチキャストアドレスを指定すれば誰でも簡単にそのストリームコンテンツを利用できる為、利用資格を有する特定の利用者向けにコンテンツを提供しようとした場合、前記暗号化を用いないマルチキャスト

トではコンテンツの不正利用が行われるという問題があった。

【０００５】またストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで配送した場合、盗聴によるストリームコンテンツの不正利用は防御しているが、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能な為、不正利用される恐れがあるという問題があった。

【０００６】更に、暗号化コンテンツを復号化する為の鍵が、通信パケットの欠落や通信の遅延で送付されなかった場合、正当な利用者であってもストリームコンテンツを利用できない可能性があるという問題があった。

【０００７】本発明の目的は上記問題を解決し、暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能な技術を提供することにある。

【０００８】本発明の他の目的は暗号化コンテンツを復号化する為の鍵の配送をより確実に行うことが可能な技術を提供することにある。

【０００９】

【課題を解決するための手段】本発明は、コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送システムにおいて、暗号化コンテンツを復号化する為の鍵をマルチキャストで各情報利用端末に配送するものである。

【００１０】本発明の情報配送システムでは、コンテンツを暗号化または復号化する為の鍵を生成した後に、その鍵を各情報利用端末毎の暗号鍵で暗号化して暗号化鍵データを生成し、その生成した暗号化鍵データをマルチキャストで各情報利用端末に配送する。

【００１１】各情報利用端末では、前記マルチキャストで配送された暗号化鍵データを受信して当該情報利用端末内に保存しておき、マルチキャストで配送された暗号化コンテンツを受信した際に、前記情報利用端末内に保存しておいた暗号化鍵データを復号化して鍵を生成し、前記取得した暗号化コンテンツを前記生成した鍵で復号化してコンテンツを利用する。

【００１２】以上の様に本発明の情報配送システムによれば、暗号化コンテンツを復号化する為の鍵をマルチキャストで各情報利用端末に配送するので、暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能である。

【００１３】

【発明の実施の形態】以下に暗号化コンテンツを復号化する為の鍵を暗号化した後にマルチキャストで各情報利用端末に配送する一実施形態の情報配送システムについて説明する。

【００１４】図１は本実施形態の情報配送システムの概略構成を示す図である。図１に示す様に本実施形態の情報配送システムは、情報提供端末１と、情報利用端末２

～４と、鍵提供端末５とを有している。

【００１５】情報提供端末１は、ストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで情報利用端末２～４に配送する装置である。情報利用端末２～４は、情報提供端末１から配送された暗号化コンテンツをマルチキャストで鍵提供端末５から配送された鍵で復号化して利用する装置である。鍵提供端末５は、暗号化コンテンツを復号化する為の鍵をマルチキャストで情報利用端末２～４に配送する装置である。

【００１６】本実施形態において、情報提供端末１と情報利用端末２～４と鍵提供端末５は、それぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末２～４に配送する情報提供端末１と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末５とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。

【００１７】図２は本実施形態の情報提供端末１の概略構成を示す図である。図２に示す様に本実施形態の情報提供端末１は、ＣＰＵ２０１と、メモリ２０２と、磁気ディスク装置２０３と、入力装置２０４と、出力装置２０５と、ＣＤ－ＲＯＭ装置２０６と、通信装置２０７とを有している。

【００１８】ＣＰＵ２０１は、情報提供端末１全体の動作を制御する装置である。メモリ２０２は、情報提供端末１全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置２０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【００１９】入力装置２０４は、ストリームコンテンツをマルチキャストで各情報利用端末へ配送する為の各種入力を行う装置である。出力装置２０５は、ストリームコンテンツの配送に伴う各種出力を行う装置である。

【００２０】ＣＤ－ＲＯＭ装置２０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。通信装置２０７は、インターネットやイントラネット等のネットワークを介して各情報利用端末及び鍵提供端末５との通信を行う装置である。

【００２１】また情報提供端末１は、鍵取得部２１１と、鍵保存部２１２と、コンテンツ暗号化部２１３と、コンテンツ配送部２１４とを有している。

【００２２】鍵取得部２１１は、利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末５から取得する処理部である。鍵保存部２１２は、鍵取得部２１１によって取得された鍵をメモリ２０２または磁気ディスク装置２０３に保存する処理部である。

【００２３】コンテンツ暗号化部２１３は、鍵保存部２１２によってメモリ２０２または磁気ディスク装置２０

3に保存された鍵によりコンテンツを暗号化する処理部である。コンテンツ配送部214は、コンテンツ暗号化部213によって暗号化されたコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送する処理部である。

【0024】情報提供端末1を鍵取得部211、鍵保存部212、コンテンツ暗号化部213及びコンテンツ配送部214として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0025】図3は本実施形態の情報利用端末2の概略構成を示す図である。図3に示す様に本実施形態の情報利用端末2は、CPU301と、メモリ302と、磁気ディスク装置303と、入力装置304と、出力装置305と、CD-ROM装置306と、通信装置307とを有している。

【0026】CPU301は、情報利用端末2全体の動作を制御する装置である。メモリ302は、情報利用端末2全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置303は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【0027】入力装置304は、マルチキャストで情報提供端末1から配送されたストリームコンテンツを取得する為の各種入力を行う装置である。出力装置305は、ストリームコンテンツの取得に伴う各種出力を行う装置である。

【0028】CD-ROM装置306は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。通信装置307は、インターネットやイントラネット等のネットワークを介して情報提供端末1及び鍵提供端末5との通信を行う装置である。

【0029】また情報利用端末2は、鍵取得部311と、鍵保存部312と、コンテンツ取得部313と、識別情報確認部314と、鍵復号化部315と、コンテンツ復号化部316と、コンテンツ再生部317と、鍵変更予告取得部318と、鍵確認部319と、鍵再配送要求部320と、鍵再取得部321とを有している。

【0030】鍵取得部311は、利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データを鍵提供端末5からマルチキャストで取得する処理部である。鍵保存部312は、鍵取得部311によって取得された暗号化鍵データをメモリ302または磁気ディスク装置303に保存する処理部である。

【0031】コンテンツ取得部313は、暗号化コンテンツを情報提供端末1からマルチキャストで取得する処理部である。識別情報確認部314は、前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認する処理部である。

【0032】鍵復号化部315は、前記保存した暗号化鍵データを復号化して鍵を生成する処理部である。コンテンツ復号化部316は、コンテンツ取得部313によって取得された暗号化コンテンツを、鍵復号化部315で生成した鍵で復号化する処理部である。

【0033】コンテンツ再生部317は、コンテンツ復号化部316によって復号化されたコンテンツを再生する処理部である。鍵変更予告取得部318は、暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を取得する処理部である。

【0034】鍵確認部319は、前記取得した鍵変更予告で予告された変更後の鍵を取得しているかどうかを確認する処理部である。鍵再配送要求部320は、前記変更後の鍵を取得していない場合にその変更後の鍵の再配送を要求する処理部である。鍵再取得部321は、前記再配送を要求した変更後の暗号化鍵データを取得する処理部である。

【0035】情報利用端末2を鍵取得部311、鍵保存部312、コンテンツ取得部313、識別情報確認部314、鍵復号化部315、コンテンツ復号化部316、コンテンツ再生部317、鍵変更予告取得部318、鍵確認部319、鍵再配送要求部320及び鍵再取得部321として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0036】なお情報利用端末3及び4についても情報利用端末2の構成と同様であるものとする。

【0037】図4は本実施形態の鍵提供端末5の概略構成を示す図である。図4に示す様に本実施形態の鍵提供端末5は、CPU401と、メモリ402と、磁気ディスク装置403と、入力装置404と、出力装置405と、CD-ROM装置406と、通信装置407とを有している。

【0038】CPU401は、鍵提供端末5全体の動作を制御する装置である。メモリ402は、鍵提供端末5全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置403は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【0039】入力装置404は、コンテンツを暗号化ま

たは復号化する為の鍵をユニキャストで情報提供端末1及び各情報利用端末へ配送する為の各種入力を行う装置である。出力装置405は、コンテンツを暗号化または復号化する為の鍵の配送に伴う各種出力を行う装置である。

【0040】CD-ROM装置406は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。通信装置407は、インターネットやイントラネット等のネットワークを介して情報提供端末1及び各情報利用端末との通信を行う装置である。

【0041】また鍵提供端末5は、鍵生成部411と、鍵暗号化部412と、識別情報付加部413と、鍵配送部414と、鍵更新部415と、鍵変更予告配送部416と、鍵再配送受付部417と、鍵再配送部418とを有している。

【0042】鍵生成部411は、コンテンツを暗号化または復号化する為の鍵を生成する処理部である。鍵暗号化部412は、前記鍵を暗号化して暗号化鍵データを生成する処理部である。識別情報付加部413は、前記生成した鍵及び暗号化鍵データにそれらを識別する為の識別情報を付加する処理部である。

【0043】鍵配送部414は、鍵生成部411で生成された鍵を情報提供端末1に配送し、鍵暗号化部412で生成された暗号化鍵データをマルチキャストで各情報利用端末に配送する処理部である。鍵更新部415は、鍵配送部414から鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を情報提供端末1に指定する処理部である。

【0044】鍵変更予告配送部416は、暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を各情報利用端末に配送する処理部である。鍵再配送受付部417は、変更後の鍵の再配送要求を情報利用端末から受け付ける処理部である。鍵再配送部418は、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データを再配送する処理部である。

【0045】鍵提供端末5を鍵生成部411、鍵暗号化部412、識別情報付加部413、鍵配送部414、鍵更新部415、鍵変更予告配送部416、鍵再配送受付部417及び鍵再配送部418として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0046】なおコンテンツを暗号化または復号化する為の鍵の生成及び配送を階層化された複数の鍵提供端末5によって行い、処理負荷を分散させても良い。

【0047】本実施形態の情報提供端末1には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、鍵提供端末5から情報提供端末1及び各情報利用端末に鍵を、また情報提供端末1から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとする。なお利用資格変更に伴って鍵が更新されるものとしたり、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末1に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。

【0048】図5は本実施形態の鍵提供端末5の鍵配送処理の処理手順を示すフローチャートである。図5に示す様に鍵提供端末5は、暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データや鍵の変更を予告する鍵変更予告をマルチキャストで各情報利用端末に配送する処理を行う。

【0049】図5のステップ501で鍵提供端末5の鍵生成部411は、所定の時間が経過した場合や情報提供端末1の利用資格者DB中の利用資格が変更された場合等の暗号鍵Kを生成する条件が成立したかどうかを調べ、暗号鍵Kを生成する条件が成立した場合にはステップ502へ進む。

【0050】ステップ502では、コンテンツC(i)を暗号化する為の暗号鍵Kを生成する。暗号鍵Kとして通信時にIPsec(IP security protocol)で利用されているものを利用しても構わないものとする。

【0051】ステップ503で鍵暗号化部412は、利用資格者DBの内容を参照し、情報提供端末1から配送されるコンテンツC(i)の利用資格を持つ利用者について、その情報利用端末mの公開鍵Pmを読み出す。ここで、各情報利用端末は公開鍵暗号方式の公開鍵と秘密鍵を生成して公開鍵を鍵提供端末5に送付し、鍵提供端末5は各情報利用端末の公開鍵を保持しているものとする。また利用資格者DBにはどの情報利用端末がコンテンツの利用を許可されているかを示すデータが保持されているものとし、このデータはある間隔で更新されるものとする。

【0052】ステップ504では、前記読み出した情報利用端末mの公開鍵Pmを用いて暗号鍵Kを暗号化し、暗号化鍵データPm(K)を生成する。ここで暗号鍵Kの暗号化の際に暗号鍵Kのスクランブル処理やハッシュ処理を併用しても良い。

【0053】ステップ505では、前記利用資格を持つ全ての利用者の情報利用端末について、その公開鍵P1、P2、...、Pm、...、Pn(1≤m≤n)を用

いて暗号化鍵データ $P_1(K)$ 、 $P_2(K)$ 、...、 $P_m(K)$ 、...、 $P_n(K)$ の生成を行ったかどうかを調べ、利用資格者DB中にまだ処理を行っていないレコードがある場合にはステップ503へ戻って暗号化鍵データの生成を続行し、利用資格を持つ全ての利用者の情報利用端末への暗号化鍵データの生成を完了した場合にはステップ506へ進む。

【0054】ステップ506で識別情報付加部413は、前記生成された暗号鍵 K 及び暗号化鍵データ $P_1(K)$ 、 $P_2(K)$ 、...、 $P_m(K)$ 、...、 $P_n(K)$ に識別情報 i を付加して鍵配送部414へ渡す。この識別情報はIPsecのSA(Security Association)に含まれる情報を利用しても構わないものとする。

【0055】ステップ507で鍵配送部414は、前記生成された暗号鍵 $K(i)$ をユニキャストで情報提供端末1へ配送すると共に、前記生成された暗号化鍵データ $P_1(K(i))$ 、 $P_2(K(i))$ 、...、 $P_m(K(i))$ 、...、 $P_n(K(i))$ をマルチキャストで各情報利用端末へ配送する。ここで前記生成された全暗号化鍵データのある数毎に分割して送信しても良い。

【0056】ステップ508で鍵変更予告配送部416は、現在使われている暗号鍵 $K(i-1)$ が暗号鍵 $K(i)$ に変更されることを予告する鍵変更予告 $Y(i)$ をマルチキャストで各情報利用端末に配送する。

【0057】ステップ509で鍵再配送受付部417は、変更後の暗号鍵 $K(i)$ の再配送要求を情報利用端末から受信しているかどうかを調べ、変更後の暗号鍵 $K(i)$ の再配送要求を受信している場合にはステップ510へ進む。

【0058】ステップ510では、利用資格者DBの内容を参照し、前記変更後の暗号鍵 $K(i)$ の再配送要求が、利用資格を持つ利用者の情報利用端末から送信されていることを確認した後、その情報利用端末の公開鍵 P_m を読み出して暗号化鍵データ $P_m(K(i))$ を再生成する。

【0059】ステップ511で鍵再配送部418は、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データ $P_m(K(i))$ を再配送する。この際、マルチキャストで再配送を行っても良いし、ユニキャストで直接情報利用端末 m に配送しても構わないものとする。

【0060】ステップ512では、利用資格を持った全ての利用者に対する暗号鍵 $K(i)$ の配送が完了したことを示す鍵配送完了通知を鍵更新部415に伝え、ステップ513で鍵更新部415は、配送が完了した暗号鍵 $K(i)$ を次の暗号化処理で使用する鍵として決定し、その暗号鍵 $K(i)$ の識別情報 i 或いは暗号鍵 $K(i)$ そのものの情報を情報提供端末1のコンテンツ暗号化部213に通知してステップ501へ戻る。

【0061】前記の様に本実施形態の情報配送システムでは、暗号化コンテンツを復号化する為の鍵をマルチキ

ャストで各情報利用端末に配送しているので、複数の情報利用端末への鍵の配送を効率的に行うことが可能である。

【0062】図6は本実施形態の各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。図6に示す様に各情報利用端末は、暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データを鍵提供端末5からマルチキャストで取得する処理を行う。また鍵変更予告で予告された変更後の鍵を取得していない場合にはその変更後の鍵の再配送を要求する処理を行う。

【0063】図6のステップ601で情報利用端末 m の鍵取得部311は、鍵提供端末5からマルチキャストで暗号化鍵データ $P_1(K(i))$ 、 $P_2(K(i))$ 、...、 $P_m(K(i))$ 、...、 $P_n(K(i))$ を受信しているかどうかを調べ、暗号化鍵データを受信している場合にはステップ602へ進み、前記受信した暗号化鍵データの中からその情報利用端末 m の公開鍵 P_m で暗号化された暗号化鍵データ $P_m(K(i))$ を取得して鍵保存部312に渡す。

【0064】ステップ603で鍵保存部312は、鍵提供端末5の識別情報付加部413によって付加された識別情報 i を暗号化鍵データ $P_m(K(i))$ から読み出し、ステップ604では、ステップ602で取得した暗号化鍵データ $P_m(K(i))$ をステップ603で読み出した識別情報 i 毎に分類してメモリ302または磁気ディスク装置303に保存する。ここで各情報利用端末が暗号鍵 $K(i)$ を磁気ディスク装置303に保存する場合には暗号化鍵データ $P_m(K(i))$ を復号化した暗号鍵 $K(i)$ を保存することとしても良い。

【0065】ステップ605で鍵変更予告取得部318は、現在使われている暗号鍵 $K(i-1)$ が暗号鍵 $K(i)$ に変更されることを予告する鍵変更予告 $Y(i)$ を鍵提供端末5から受信しているかどうかを調べ、鍵変更予告 $Y(i)$ を受信している場合にはステップ606へ進む。

【0066】ステップ606で鍵確認部319は、前記取得した鍵変更予告 $Y(i)$ で予告された変更後の暗号鍵 $K(i)$ を取得しているかどうかを調べ、鍵変更予告 $Y(i)$ に示された識別情報 i の暗号化鍵データ $P_m(K(i))$ がメモリ302または磁気ディスク装置303に保存されていない場合にはステップ607へ進む。

【0067】ステップ607で鍵再配送要求部320は、前記変更後の暗号鍵 $K(i)$ の再配送を鍵提供端末5に要求する。ステップ608で鍵再取得部321は、前記再配送を要求した変更後の暗号化鍵データ $P_m(K(i))$ を鍵提供端末5から受信してメモリ302または磁気ディスク装置303に保存する。

【0068】前記の様に本実施形態の情報配送システムでは、暗号化コンテンツの鍵が変更されることを予告す

る鍵変更予告を鍵提供端末5から各情報利用端末に送信し、鍵の再配送を行っているので、暗号化コンテンツを復号化する為の鍵が、マルチキャストの際の通信パケットの欠落や通信の遅延で送付されなかった場合に鍵を再配送し、正当な利用者が確実にストリームコンテンツを利用できる様にしている。

【0069】図7は本実施形態の情報提供端末1のコンテンツ配送処理の処理手順を示すフローチャートである。図7に示す様に情報提供端末1のコンテンツ暗号化部213は、鍵取得部211により鍵提供端末5から取得し鍵保存部212によって保存された鍵の内、鍵提供端末5の鍵更新部415により指定された識別情報*i*の暗号鍵*K*(*i*)を用いてコンテンツ*C*(*i*)を暗号化し、前記暗号化されたコンテンツである暗号化コンテンツ*K*(*i*)(*C*(*i*))をコンテンツ配送部214によりマルチキャストで各情報利用端末に配送する処理を行う。

【0070】図7のステップ701で情報提供端末1のコンテンツ暗号化部213は、鍵保存部212によってメモリ202または磁気ディスク装置203に保存されていた鍵の内、鍵提供端末5の鍵更新部415により指定された識別情報*i*の暗号鍵*K*(*i*)を読み出す。

【0071】ステップ702では、配送対象のコンテンツ*C*(*i*)を所定の単位で読み出し、ステップ703では、ステップ702で読み出したコンテンツ*C*(*i*)のデータをステップ701で読み出した暗号鍵*K*(*i*)で暗号化して暗号化コンテンツ*K*(*i*)(*C*(*i*))を生成し、コンテンツ配送部214に渡す。ここで暗号化の単位はネットワーク配送を行う為のパケットの大きさを単位としても構わないものとする。またコンテンツの暗号化の際にコンテンツのスクランブル処理やハッシュ処理を併用しても良い。

【0072】ステップ704でコンテンツ配送部214は、前記生成された暗号化コンテンツ*K*(*i*)(*C*(*i*))のヘッダー等に暗号鍵*K*(*i*)の識別情報*i*を付加する。なおここでIPsecのヘッダーを利用しても構わないものとする。

【0073】ステップ705では、前記識別情報*i*の付加された暗号化コンテンツ*K*(*i*)(*C*(*i*))をマルチキャストで情報利用端末2~4へ配送する。ステップ706では、配送対象のコンテンツ*C*(*i*)について全てのデータを情報利用端末2~4に配送したかどうかを調べ、まだ配送を行っていないデータがある場合にはステップ702へ戻ってコンテンツ*C*(*i*)の配送を続行し、全データの配送を完了した場合にはコンテンツ*C*(*i*)の配送処理を終了する。

【0074】図8は本実施形態の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。図8に示す様に各情報利用端末は、マルチキャストで配送された暗号化鍵データを復号化して生成した鍵を

用いて暗号化コンテンツを復号化する処理を行う。

【0075】図8のステップ801で各情報利用端末のコンテンツ取得部313は、情報提供端末1からマルチキャストで暗号化コンテンツ*K*(*i*)(*C*(*i*))を受信しているかどうかを調べ、暗号化コンテンツ*K*(*i*)(*C*(*i*))を受信している場合にはステップ802へ進み、前記受信した暗号化コンテンツ*K*(*i*)(*C*(*i*))を取得して識別情報確認部314に渡す。

【0076】ステップ803で識別情報確認部314は、前記取得した暗号化コンテンツ*K*(*i*)(*C*(*i*))のヘッダー等を参照し、暗号化コンテンツ*K*(*i*)(*C*(*i*))に付加されている識別番号*i*を確認して鍵復号化部315へ通知する。

【0077】ステップ804で鍵復号化部315は、識別情報確認部314から通知されたものと同じの識別番号*i*を持つ暗号鍵*K*(*i*)の読み込みが未実行であるかどうかを調べ、暗号鍵*K*(*i*)の読み込みが未実行である場合にはステップ805へ進む。

【0078】ステップ805では、鍵保存部312によってメモリ302または磁気ディスク装置303に保存されている暗号化鍵データの内、識別情報確認部314から通知されたものと同じの識別番号*i*を持つ暗号化鍵データ*P_m*(*K*(*i*))を読み出す。ステップ806では、前記読み出した暗号化鍵データ*P_m*(*K*(*i*))を情報利用端末*m*の公開鍵*P_m*に対応する秘密鍵で復号化し、暗号鍵*K*(*i*)を生成する。

【0079】ステップ807でコンテンツ復号化部316は、ステップ802で取得した暗号化コンテンツ*K*(*i*)(*C*(*i*))をステップ806で生成した暗号鍵*K*(*i*)によって復号化してコンテンツ*C*(*i*)を生成し、ステップ807でコンテンツ再生部317は、前記復号化によって得られたコンテンツ*C*(*i*)を再生してステップ801へ戻る。

【0080】前記の様に本実施形態では、情報提供端末1から配送されるコンテンツ*C*(*i*)の利用資格を持つ利用者の情報利用端末へマルチキャストで暗号化鍵データ*P_m*(*K*(*i*))(復号兼用)を配送した後、暗号化コンテンツ*K*(*i*)(*C*(*i*))をマルチキャストで各情報利用端末へ配送しているので、コンテンツの利用資格を失った利用者による不正利用を防止しつつマルチキャストを利用した効率的なコンテンツ及び鍵の提供を行うことができる。

【0081】また前記の例では、暗号化鍵データ、鍵変更予告*Y*、暗号化コンテンツを別々に配送しているが、それらの2つ以上を同一のパケットに合成してマルチキャストで配送を行っても良い。

【0082】すなわちステップ507で鍵提供端末5の鍵配送部414は、前記生成された暗号鍵*K*(*i*)と共に暗号化鍵データ*P*1(*K*(*i*))、*P*2(*K*(*i*))、...*P_m*(*K*(*i*))、...*P_n*(*K*(*i*))、

(i)) をユニキャストで情報提供端末1へ配送する。

【0083】またステップ508で鍵変更予告配送部416は、暗号化コンテンツの暗号鍵 $K(i-1)$ が暗号鍵 $K(i)$ に変更されることを予告する鍵変更予告 $Y(i)$ をユニキャストで情報提供端末1へ配送する。

【0084】そしてステップ704で情報提供端末1のコンテンツ配送部214は、単数または複数の暗号化鍵データ(例えば $P1(K(i))$ と $P2(K(i))$)等)や、暗号鍵 $K(i-1)$ が暗号鍵 $K(i)$ に変更されることを予告する鍵変更予告 $Y(i)$ を暗号化コンテンツ $K(i-1)(C(i-1))$ の一部と同一のパケットに合成し、ステップ705でマルチキャストにより各情報利用端末へ配送する。ここで暗号化コンテンツ $K(i-1)(C(i-1))$ は、暗号鍵 $K(i)$ の前に生成された暗号鍵 $K(i-1)$ によってコンテンツ $C(i-1)$ を暗号化したものである。

【0085】各情報利用端末では、暗号化鍵データ $P1(K(i))$ 、 $P2(K(i))$ 、...、 $Pm(K(i))$ 、...、 $Pn(K(i))$ 、鍵変更予告 $Y(i)$ 、暗号化コンテンツ $K(i-1)(C(i-1))$ の内の2つ以上のデータを同一のマルチキャストにより取得し、各取得部によりそれら分離して取得する。

【0086】この様に暗号化コンテンツ $K(i-1)(C(i-1))$ と、変更後の暗号鍵 $K(i)$ の暗号化鍵データ $P1(K(i))$ 、 $P2(K(i))$ 、...、 $Pm(K(i))$ 、...、 $Pn(K(i))$ や、暗号鍵 $K(i-1)$ が暗号鍵 $K(i)$ に変更されることを予告する鍵変更予告 $Y(i)$ を同一のマルチキャストで配送することにより、コンテンツを利用している各情報利用端末に、より確実に変更後の暗号鍵 $K(i)$ を配送することができる。

【0087】また前記の例では、暗号化コンテンツを復号化する為の鍵を各情報利用端末の公開鍵で暗号化して暗号化鍵データを生成しているが、各情報利用端末と鍵提供端末5とが共有する共通秘密鍵を用いて暗号化鍵データを生成しても良い。

【0088】すなわちステップ503～ステップ505で鍵提供端末5の鍵暗号化部412は、利用資格者DBの内容を参照し、情報提供端末1から配送されるコンテンツ $C(i)$ の利用資格を持つ利用者について、その情報利用端末の共通秘密鍵 $S1$ 、 $S2$ 、...、 Sm 、...、 $Sn(1 \leq m \leq n)$ を用いて暗号化鍵データ $S1(K)$ 、 $S2(K)$ 、...、 $Sm(K)$ 、...、 $Sn(K)$ を生成する。ここで、各情報利用端末は情報利用端末または利用者の個別情報を利用して共通秘密鍵を生成して鍵提供端末5に送付しているものとする。なお前記個別情報とは、各情報利用端末が生成していた秘密鍵、媒体固有番号、IPアドレス、利用者のユーザID、パスワード、生年月日等のユーザ個人情報である。

【0089】そしてステップ806では、暗号化鍵データ $Sm(K(i))$ を情報利用端末 m の共通秘密鍵 Sm で復号化して暗号鍵 $K(i)$ を生成し、暗号化コンテンツ $K(i)(C(i))$ の復号化に用いる。

【0090】以上説明した様に本実施形態の情報配送システムによれば、暗号化コンテンツを復号化する為の鍵をマルチキャストで各情報利用端末に配送するので、暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能である。

【0091】また本実施形態の情報配送システムによれば、暗号化コンテンツの鍵が変更されることを予告し、要求に応じて鍵の再配送を行なうので、暗号化コンテンツを復号化する為の鍵の配送をより確実に行うことが可能である。

【0092】

【発明の効果】本発明によれば暗号化コンテンツを復号化する為の鍵をマルチキャストで各情報利用端末に配送するので、暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能である。

【図面の簡単な説明】

【図1】本実施形態の情報配送システムの概略構成を示す図である。

【図2】本実施形態の情報提供端末1の概略構成を示す図である。

【図3】本実施形態の情報利用端末2の概略構成を示す図である。

【図4】本実施形態の鍵提供端末5の概略構成を示す図である。

【図5】本実施形態の鍵提供端末5の鍵配送処理の処理手順を示すフローチャートである。

【図6】本実施形態の各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。

【図7】本実施形態の情報提供端末1のコンテンツ配送処理の処理手順を示すフローチャートである。

【図8】本実施形態の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。

【符号の説明】

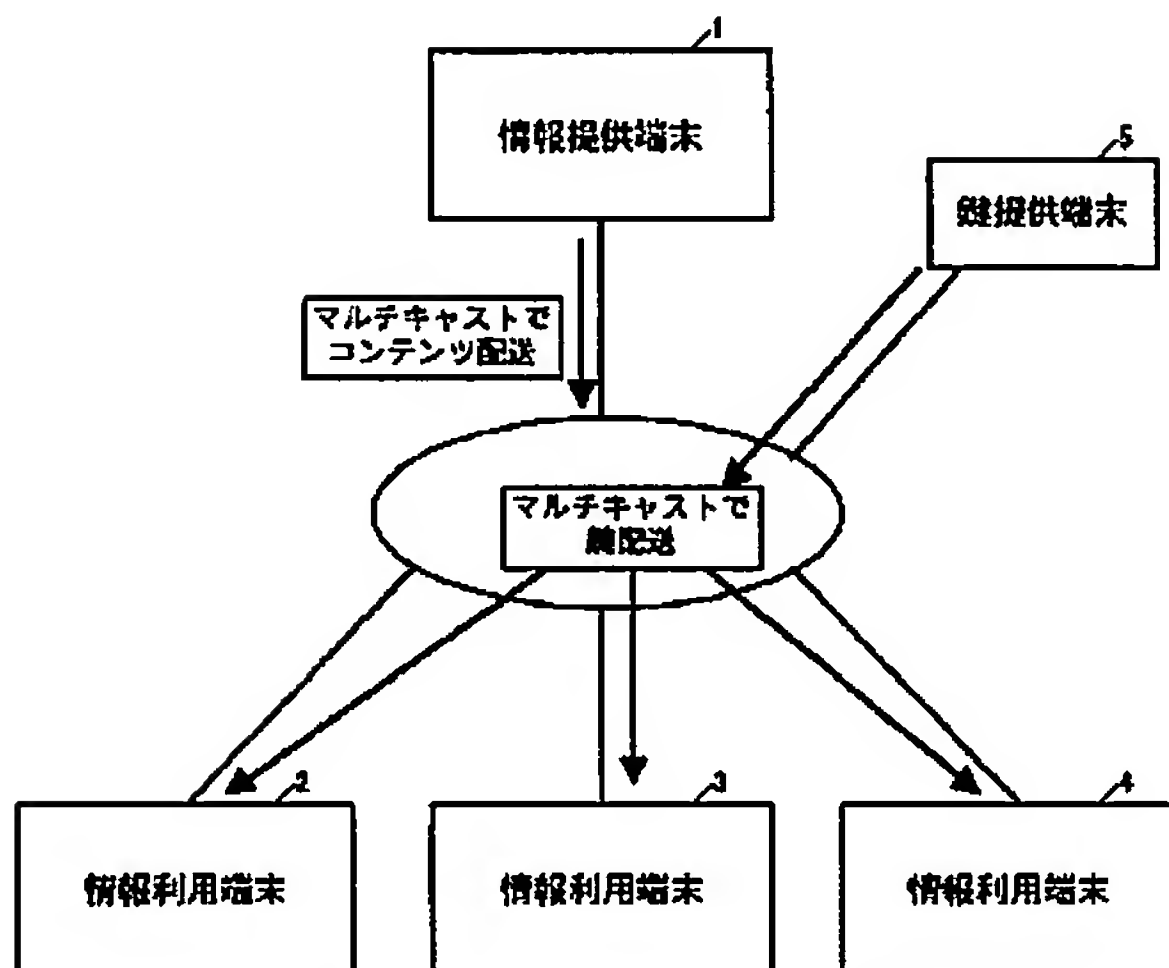
1…情報提供端末、2～4…情報利用端末、5…鍵提供端末、201…CPU、202…メモリ、203…磁気ディスク装置、204…入力装置、205…出力装置、206…CD-ROM装置、207…通信装置、211…鍵取得部、212…鍵保存部、213…コンテンツ暗号化部、214…コンテンツ配送部、301…CPU、302…メモリ、303…磁気ディスク装置、304…入力装置、305…出力装置、306…CD-ROM装置、307…通信装置、311…鍵取得部、312…鍵保存部、313…コンテンツ取得部、314…識別情報確認部、315…鍵復号化部、316…コンテンツ復号化部、317…コンテンツ再生部、318…鍵変更予告取得部、319…鍵確認部、320…鍵再配送要求部、

321…鍵再取得部、401…CPU、402…メモリ、403…磁気ディスク装置、404…入力装置、405…出力装置、406…CD-ROM装置、407…通信装置、411…鍵生成部、412…鍵暗号化部、4

13…識別情報付加部、414…鍵配送部、415…鍵更新部、416…鍵変更予告配送部、417…鍵再配送受付部、418…鍵再配送部。

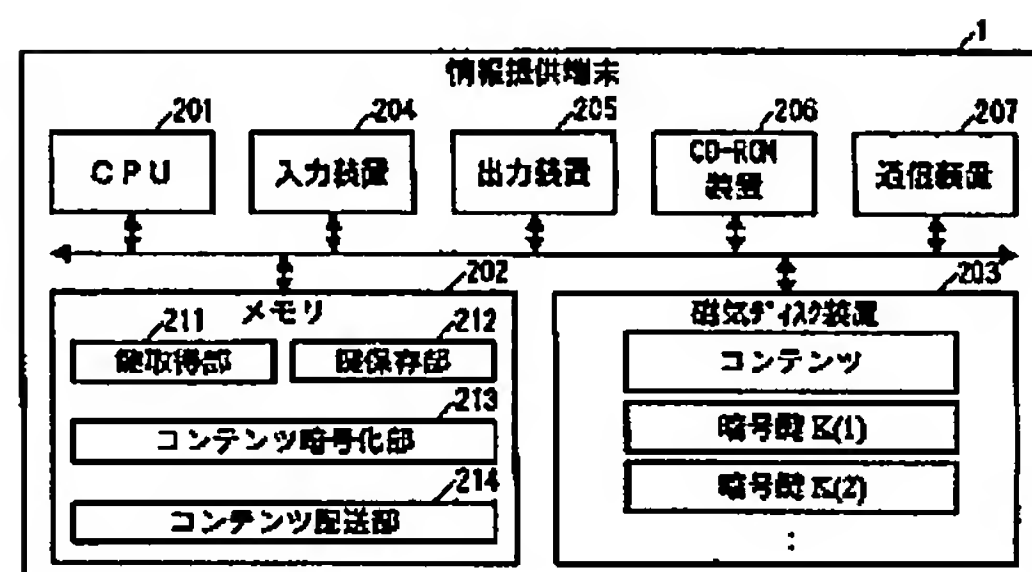
【図1】

図1



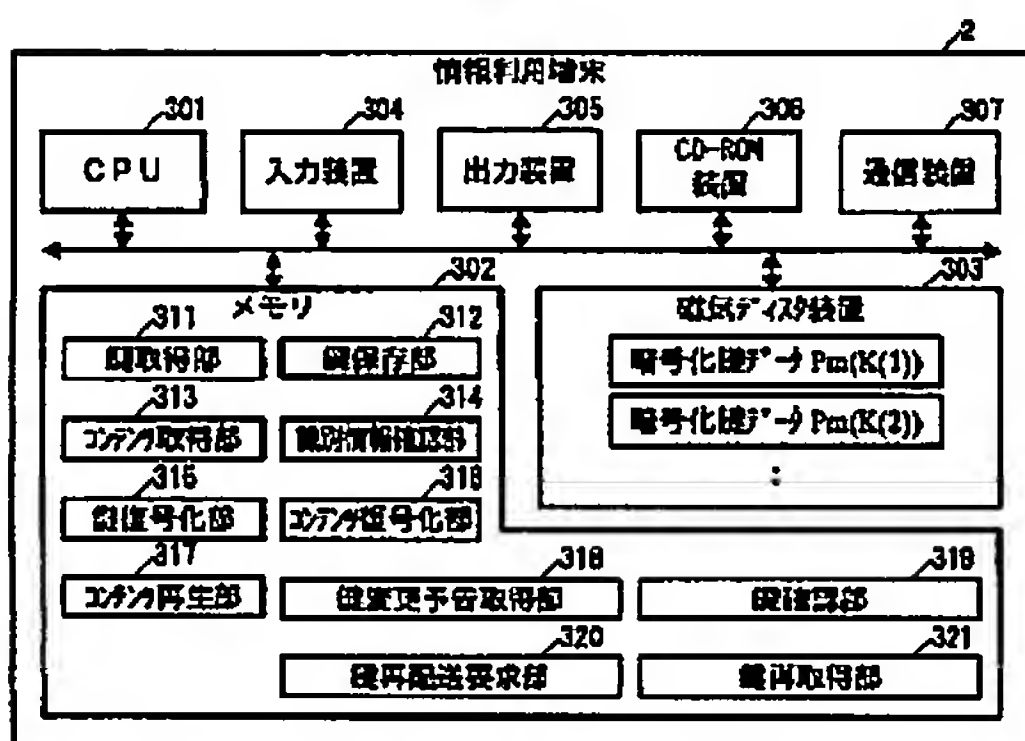
【図2】

図2



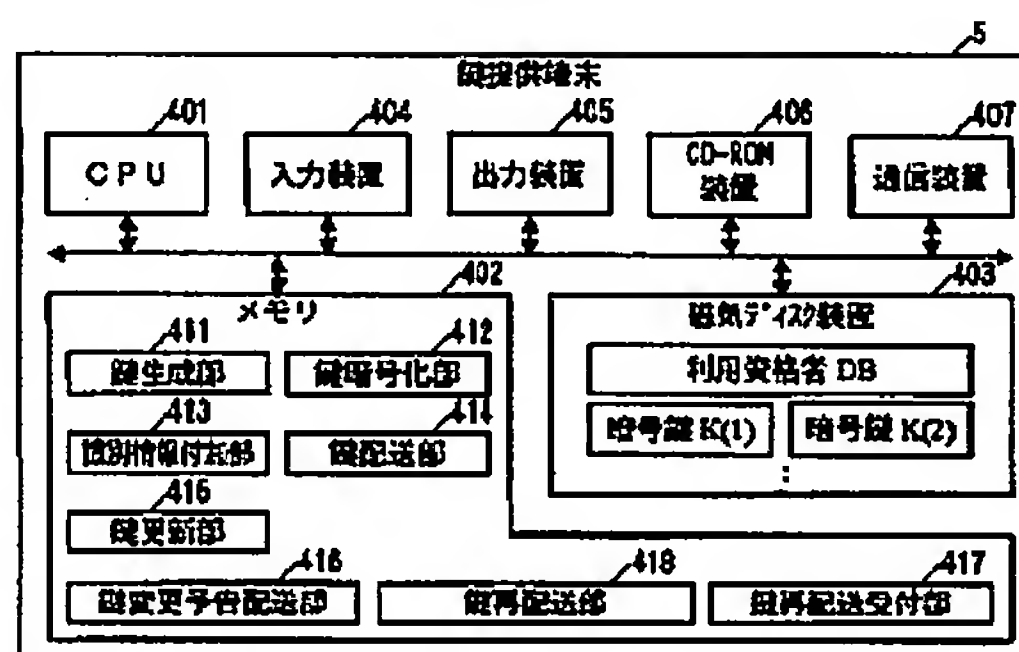
【図3】

図3

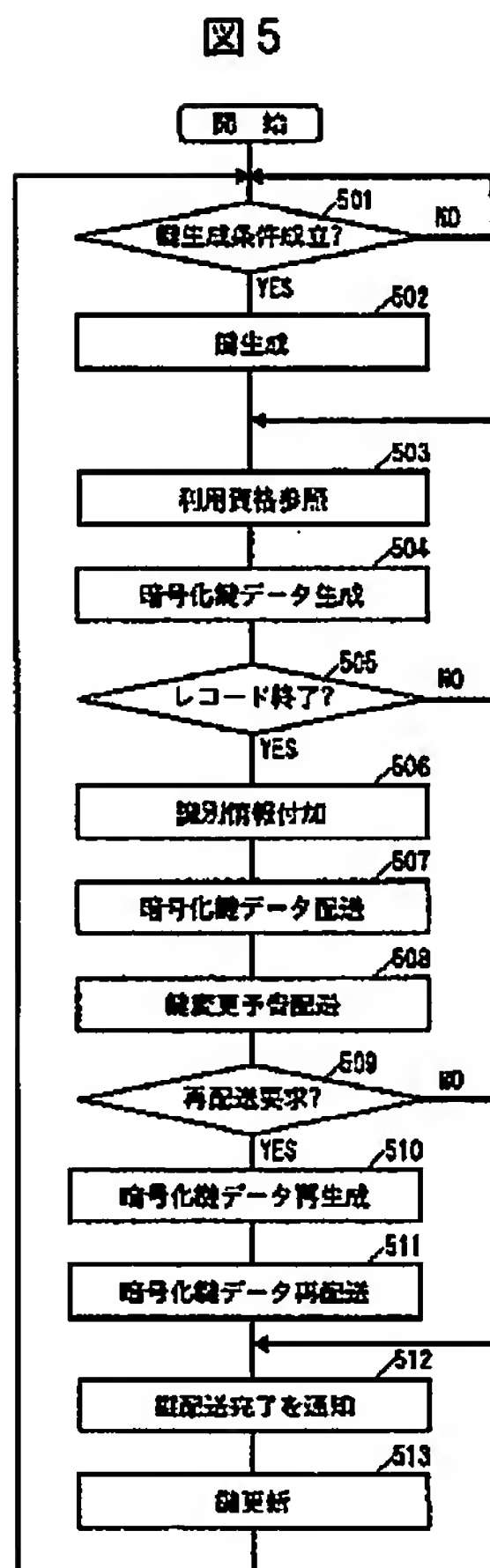


【図4】

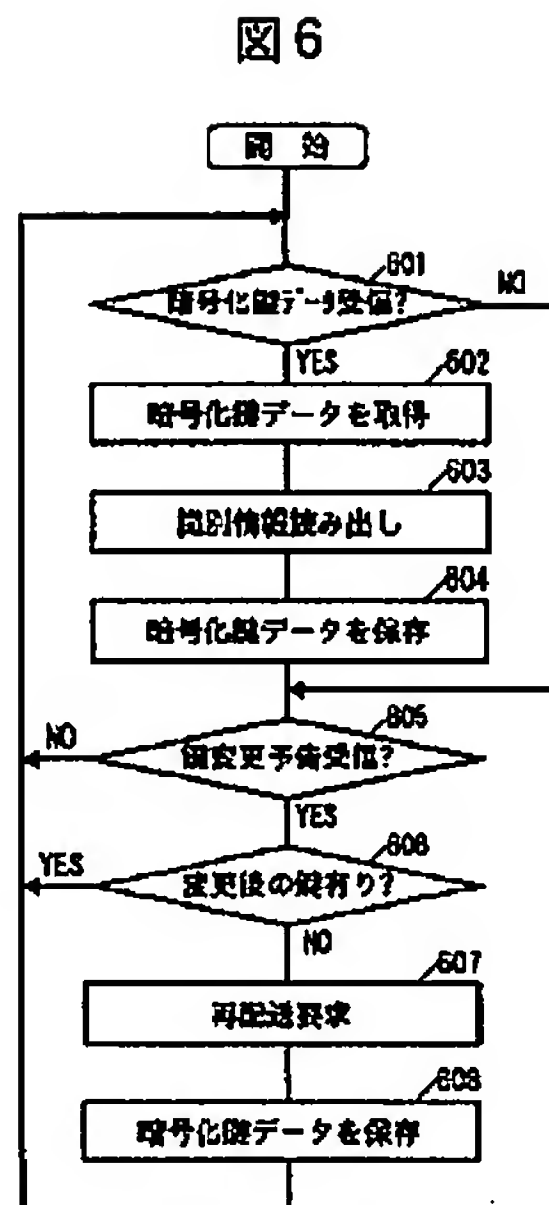
図4



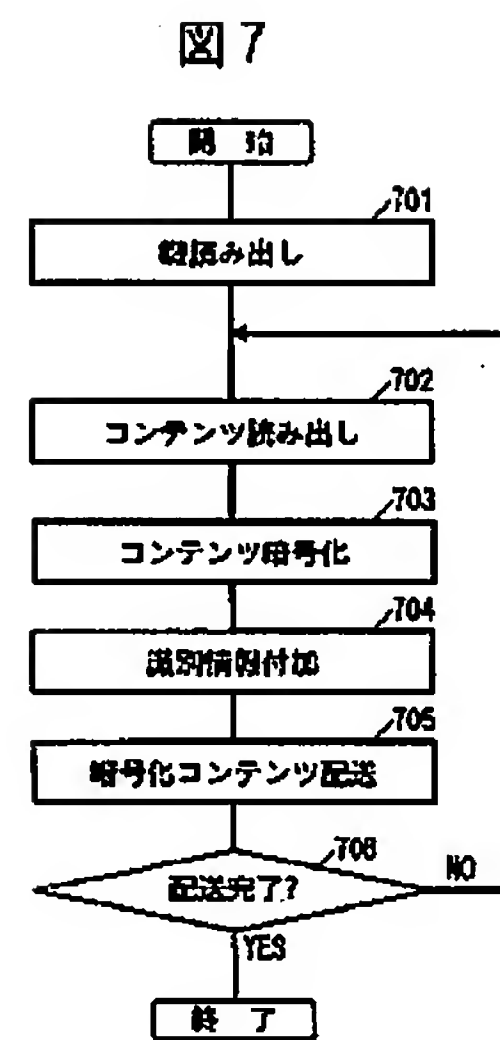
【図5】



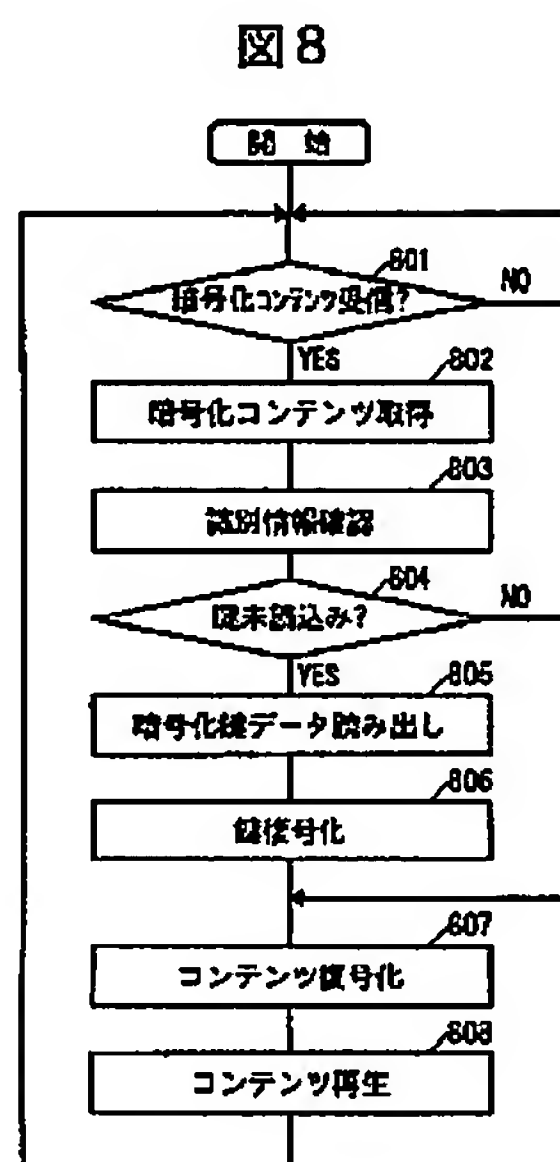
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 中里 加奈
東京都千代田区大手町二丁目 3 番 1 号 日
本電信電話株式会社内

Fターム(参考) 5J104 AA01 AA16 BA03 EA01 EA04
EA17 NA02 PA04 PA05